International Journal of Humanities and Social Sciences (IJHSS)
ISSN (P): 2319–393X; ISSN (E): 2319–3948
Vol. 10, Issue 2, Jul–Dec 2021; 241–254

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

IDENTITY CRIME AND IT'S FORMS – STUDY OF THE RELATED LAWS IN THE UNITED KINGDOM, UNITED STATES OF AMERICA AND INDIA

***Amonkar Vassudev Anant Sinai*[1] *& Dr. Nagesh Sadanand Colvalkar*[2]**

[1]*Research Scholar, V. M. Salgaokar College of Law, Miramar, Pananji, Goa, India*

[2]*Research Guide, Professor, V. M. Salgaokar College of Law, Miramar, Pananji, Goa, India*

ABSTRACT

This article attempts to understand the premise of Identity Crime in the sense of its two main varieties i.e. Identity Theft and Identity Fraud, and seeks to consider the prevailing legal provisions that determine the violation of Identity Theft and Identity Fraud.

In the present modern age of Internet and Digitalisation where consciously and more often unknowingly, a lot of personal information of individuals is disclosed which is collected, stored and used. The information regarding identity of an individual has become a very valuable commodity presently often leading to crimes of theft and/or fraud of the individuals' very identity.

It is against this backdrop that this article attempts to examine Identity Crime and look at the related legal provisions existing primarily in the United Kingdom, the United States of America and India. For this purpose the present article has used secondary data from books, articles, journals, newspapers, online publications, etc.

KEYWORDS: *Identity Crime, Identity Theft, Identity Fraud, Data Protection, Privacy, Digitalisation*

Article History

Received: *04 Oct 2021* **|** ***Revised:*** *07 Oct 2021* **|** ***Accepted:*** *13 Oct 2021*

INTRODUCTION

Today we all literally exist in the world of "*Digitalisation*" steered in by the advent of "Internet".

The strong impact of the present day digital technologies is rampant in every spectrum of our lives and accordingly the current era is also rightly termed as the "*Digital Age*". Today Digitalisation can be viewed as a tool of change which transcends beyond our lifestyle to say the way we transact, interact and even conduct business. The landscape of this Digital Age is progressively driven by advancement in e-communications, e-commerce and ever increasing use of the internet to build economies based on high technology, massive communication, knowledge creation and innovation".[1]

The easy accessibility of the information and its technological capacity has opened new avenues to use, and more often misuse and abuse the technology either through cheating, fraud and such similar crimes. The information shared over the internet consciously and more often unknowingly is getting used by computing systems to collect, analyse and interpret large amounts of individual personal information. The opportunity of exploiting personal information is combined with

[1] http://www.mazars.co.in/Home/News/Our-Publications/Digitalisation

intricacy and exposure to various vulnerabilities which the individual may have to face which can extend to significant economic consequence, cyber terrorism & attacks, etc.

Technology has made it possible to shape and create several new hand - held devices including mobile, wireless internet access tools, remote access tools, etc, giving new impetus for exploiting personal information in the form of data, and this data can be altered, destroyed, tampered, stolen, repudiated, etc.

In the present day and age a key area of misuse of an individual's personal information or data across the world is of "*Identity Theft* ".

Identity Theft has thus today become an increasingly common problem also in India, as fraudsters learn newer and innovative ways to procure the personal information which is required to steal someone's identity.

Identity theft rarely involves the unauthorised taking of a victim's personal physical possessions, however what it does involve is the perpetrator of the crime taking the victim's personal information or data and then using this in an illegal and unlawful way for their own personal gain".[2]

Identity theft happens when perpetrator accesses sufficient information about someone's identity (such as the name, date of birth, current or previous addresses, etc) to commit an identity crime or identity fraud. Surprisingly such Identity theft can occur even when the fraud victim is deceased.

When an individual becomes a victim of identity theft, it mostly then leads to fraud that can have serious and direct impact on the victim's personal finances".[3]

Identity theft thus can be said to be a sub set of "Data Theft" in which personal information of an individual forms the stolen data and is the medium to perpetrate several other crimes. Identity Theft thus has emerged to be one of the fastest growing crimes in several countries across the globe including in India".[4]

UDERSTANDING IDENTITY THEFT AND IDENTITY FRAUD:-

Identity Theft

In general terms "Identity Theft" can be understood to consist of all types of crimes wherein an individual fraudulently obtains another individual's personal information and uses it mainly for economic gain".[5]

"Identity Theft" can thus be termed as, the unlawful use of someone else's personal information particularly in order to obtain money or credit.[6] It is can also be understood as, the act of stealing an individual's personal identifying information in order to access tha individual's financial resources, or access certain other benefits, such as money, credit, or insurance benefits. Also, the act of deceitfully obtaining and using another individual's identifying or personal financial documents, such as a credit card or bank account, generally for the purpose of financial gain[7] constitutes Identity Theft.

[2] http://www.identitytheft.org.uk/
[3] https://www.actionfraud.police.uk/
[4] Vivek Tripathi, Cyber Laws India Cyberlawsindia.net, http://www.cyberlawsindia.net/index1.html
[5] Berni Dwan, *Identity theft*, 2004 Computer Fraud & Security 14-17 (2004).
[6] https://www.merriam-webster.com/dictionary/identity%20theft
[7] https://legaldictionary.net/identity-theft/

Identity Theft therefore can be said to include use of fraud or cheating methods to obtain someone else's identity information so as to use such information to access financial information or to obtain credit and other benefits in that individual's name".[8]

Identity Fraud

"Identity Fraud" can be understood as a crime in which a fraudster obtains certain important pieces of another person's personally identifiable information, such as Mobile Number, PAN Card Number, Aadhar Card Number or Driver's License number, in order to impersonate that individual. This critical personal information can be then potentially used to access the individual's personal finances, obtain credit, shop for merchandise and services online, all in the name of that individual, or even used to provide the fraudster with false credentials.

In certain rare cases, the fraudster may even provide false identification to police, create a false criminal record or leave arrest warrants in the name of the individual whose identity has been stolen".[9]

Identity Fraud can also be understood as, the illegal use of another individual's personal details, in order to siphon or steal money from their bank account.[10] Identity Fraud thus is a crime in which the fraudster obtains and uses a victim's personal information through fraud or deceit primarily for economic gain.[11]

Identity fraud can also be understood as the use of stolen identity in a criminal act to obtain financial gain, goods or services by means of deception. The fraudsters may use the victim's personal identity details to:

- Access bank accounts.
- Obtain credit cards, loans etc.
- Carry out online shopping of goods in the name of the victim.
- Gain control of existing Bank accounts of the victim.
- Access mobile phone and social media contacts of the victim.
- Obtain documents such as passport or driving licence in the name of the victim.

Interestingly, stealing an individual's identity details *per-se* may not on its own constitute identity fraud, but *using* that stolen identity to commit or perpetrate illegal activity does would".[12]

DISTINCTION BETWEEN IDENTITY THEFT AND IDENTITY FRAUD:

Generally, people tend to use the terms Identity Theft and Identity Fraud interchangeably, but there are certain very important differences between these two. Since information is one of the best ways to prevent becoming a victim of either crime, it's in the best interest to know these differences.

[8] Larry J. Siegel, E-Study Guide For: Criminology: Theories, Patterns, and Typologies (11 Ed. 2014).
[9] http://searchsecurity.techtarget.com/definition/identity-theft
[10] https://dictionary.cambridge.org/dictionary/english/identity-theft
[11] http://www.businessdictionary.com/definition/identity-fraud.html
[12] https://www.actionfraud.police.uk/ID

The important points of distinctions between Identity Theft and Identity Fraud are as under:

Manner of Use of Information

Fraudsters who carry out Identity Theft use an unsuspecting individual's personal information viz; PAN or Aadhar Card number, birth date, name and address to assume identity of such individual. Once this information is obtained, the fraudster may open new Bank account using this information or use the information to create a fake identity.

In the United States, as per the Department of Justice, Identity Fraud occurs when fraudsters use an individual's personal information without the person's knowledge to commit crimes, ranging from financial offences to more serious acts. This may include illegal use of credit card to make fraudulent purchases online or commit crime under the individual's name. Thus, in short, the difference between the two lies in how the information is used.

Identity Fraud is Often the Consequence of Identity Theft

Identity fraud becomes difficult crime to commit without first obtaining an individual's personal information. This means that in order for a fraudster to commit Identity Fraud the victim's personal information has to be accessed or obtained first, which act is considered as Identity Theft. Thus, Identity Fraud can be said to be a consequence of Identity Theft.

Certain Other Types of Frauds are Possible without Resorting to Identity Theft

Identity Fraud is a type of crime that results from obtaining the individual's personal information without consent to commit a crime. However, fraudsters do not always have to obtain the individual's personal information to commit certain other types of fraud, such as financial scams. Fraudsters may create personal information about a person who does not exist, and use this information to set up financial accounts with lenders, merchants and also with financial institutions. These types of crimes may be generally perpetrated by individuals or by group of fraudsters.

Nature of Victims

Victims of Identity Theft may include the person, who had his or her personal information stolen, as well as the merchants, utilities, and/or other businesses deceived by the perpetrator. On the other hand, victims of Identity Fraud may include the lenders, credit card companies, merchants, and/or such other organisations,.

Identity Theft and Identity Fraud are thus versatile crimes that may involve many legal and financial components. For this reason, understanding the different types of crimes that fall within the description of Identity Theft or Identity Fraud as the case may be or relate to these crimes can be tricky. But knowing and understanding how these crimes work separately or in combination with each other can exhibit a better on how such fraudsters operate".[13]

NEW FORMS OF IDENTITY CRIME

As social media networking bridges the gap between online and offline identities, criminals may commence exploiting the many new forms of such identity that previously may have existed but are becoming more prominent and relevant today and are even acquiring exchangeable value.

[13] https://www.freecreditscore.com/blog/identity-theft-identity-fraud/

Some of the new forms of identity crime are:

- **Social Media Friendship Identity:** This consists of exploiting friendship links on social media or chats that give access to social groups;
- **Financial Identity:** this includes exploiting an individual's information that give access to financial resources;
- **Professional Identity:** this includes exploiting access of an individual to a professional community and its clients or client database;
- **Organisational Identity:** this includes exploiting an unsuspecting employee's access to organisational resources;
- **Sexual Identity:** this includes exploiting personal information of an individual that depict sexual orientation of the individual; and;
- **Geographic Identity:** this includes exploiting location specific information to see, for example, whether an individual is not at home or away in order to steal from them.

TYPES OF IDENTITY THEFT IN INDIA

Identity theft is rampant in USA, while in India the cases of identity theft are emerging and are comparatively low given the less number of people doing online transactions and limited spread of internet. In India while there is no consistent statistics available on the extent of identity theft, it would be safe to assume a rapid rise in identity theft cases with increase in the number of online banking, financial and ecommerce transactions and due to the fact that the customers are not much technically adept with the virtual world.

Fraudulent Online Share & Commodity Transactions

Presently the shares of companies are required to be sold and purchased online. This has led to rise in cases in where a customer's online share/commodity account has been compromised and fraudulent transaction has been executed by fraudsters resulting in financial loss to the customer.

Bank Account Phishing scams

Phishing is the presently one of the internet's biggest identity theft scam widely prevalent in India. In some recent instances of phishing reported in India. Phishing is a technique of extracting confidential information such as credit card number and username and password by masquerading as a legitimate enterprise. it is typically carried out by email containing spoofed links to legitimate appearing websites.

Also not all phishing is done via email or web sites. Nowadays Phishing is done over phone calls, this is termed as "Vishing" (voice phishing) and involves calls to victims using fake identity fooling the victim into considering the call to be from a trusted source or organisation.

Nigerian 419 Scam or Advance Fee Fraud

There have been number of instances reported in India where the perpetrators send email to the victim, masquerading as a Royal Prince or wealthy businessman and requesting the help of the victim for retrieving blocked funds in return for a heavy percentage of these funds as commission. The victim believing the fraudsters and lured of receiving huge commission pass on their credit card information, bank account details to fraudster, which is then used to cause huge financial loss to the victim.

Defamation or Posting of Porn or Obscene Material on Social Networking Sites

There has also been cases in India in recent times in which the victim's social media profile and personal information is either compromised or stolen and a fake & vulgar profile in the name of the victim containing pornography & obscene material at times along with the victim's contact details like phone numbers & address posted on the social networking site resulting in defamation and mental trauma to the victim..

LAWS GOVERNING IDENTITY CRIME

United Kingdom (UK)

Some of the important legislations governing the offence of Identity Crime in the UK are mentioned briefly as follows:

Computer Misuse Act, 1990

The Computer Misuse Act (CMA), 1990 is one of the important legislation in the UK relating to the offences or attacks against computer systems such as hacking or denial of service.

The CMA interestingly does not define what is meant by a 'Computer', presumably to allow for technological development. Thus even a mobile smart-phone or personal tablet device can be defined as a "Computer" in the same way as a traditional 'desk-top' computer or "Laptop". The jurisdiction to prosecute all CMA offences UK arises if there is "at least one significant link with the domestic jurisdiction" (i.e. England and Wales) in the circumstances of the case.

Regulation of Investigatory Powers Act, 2000

The Regulation of Investigatory Powers Act (RIPA) is another important piece of legislation relating to the Identity Crime in the UK. It is important to note that under this Act, it is an offence for a person intentionally and without lawful authority to intercept, at any place within the UK, any communication in the course of its transmission by means of a public telecommunication system.

The Act also makes it an offence for a person to intercept any communication in the course of its transmission by means of any private telecommunication system.

In the United Kingdom RIPA would usually be used if the material was unlawfully intercepted during the course of its transmission and the Computer Misuse Act (CMA) would be used when the material is acquired through unauthorised access to a computer.

Data Protection Act 1998

The Data Protection Act (DPA) is an important comprehensive piece of legislation governing Identity Crime in the UK. The Data Protection Act provides for inclusion of criminal offences that may be committed alongside other cyber-dependent crimes.

These Include

- Obtaining or disclosing personal data;
- Procuring the disclosure of personal data;
- Selling or offering to sell personal data.

As identity theft involves information being stolen about a person, the DPA is the main piece of legislation in the UK that can be used in the circumstances of the case.

The (European Union) General Data Protection Regulation, 2018

The EU General Data Protection Regulation (EU-GDPR) applies to all nations and organisations that process the personal data of European resident's. Under the GDPR, businesses that fail to comply with the regulations of GDPR and suffer data breach may face fines of upto €20 million or upto 4% of its global revenue – whichever is higher.

The GDPR provides for robust limits and restrictions on the organisations on the use and store personal data or personally identifiable information of European resident's.

The Fraud Act 2006

The Fraud Act, 2006 has two relevant pieces of legislation which can be said to be related to identity crime. Firstly, dishonestly making a false representation to make a gain for oneself or another or to cause loss to another or to expose another to a risk of loss[14] is considered to be an offence. Secondly, Possession of articles for use in frauds (amongst other items), cloned credit cards is also considered to be an offence. [15]

Under the Fraud Act, identity related offences such as possessing phishing kits, using stolen credit card information, road accident fraud, benefit fraud, false information about houses (false claims), mortgage fraud, etc are considered to be offences.

The Identity Documents Act, 2010 (formerly the Identity Cards Act 2006)

The Identity Documents Act,2006 (IDA) makes it an offence for possessing or controlling a false or improperly obtained Identity Card or an identity card which relates to another person, or possesses any apparatus etc,for making false ID cards"[16].

The Malicious Communications Act 1988

The Malicious Communications Act, 1988 (MCA) though does not contain any specific provisions pertaining to Identity Crime as such, it however does provide for the offence of Cyber-bullying, which in most cases is conducted by creating fake or wrong identities[17], mostly on social media.

The United States of America (USA): Some of the important legislations governing the offence of Identity Crime in the USA are mentioned briefly as follows:

Identity Theft and Assumption Deterrence Act, 1998

The Identity Theft Assumption Deterrence Act, 1998 (ITADA) has made identity theft a crime in the USA. Under this Act, identity theft includes any misuse of identification documents or information, including Social Security number, name, or even an account number and password. The punishments under ITADA depend on the crime and the level to which it is committed. For relatively minor offence, the individual can face up to three years in prison. The punishment becomes more severe if the fraudster gained over USD$1,000 in compensation from creating such false identification documents in a one-year period. At this level, a 15-year jail sentence may be provided. Further, the fraudster can receive 20 or even 25 years in prison if the false documents that were created were used to commit a violent crime or drug trafficking.

[14] Fraud Act 2006 sections 1(2a), (3) & (4) & 2.
[15] Fraud Act 2006, section 6.
[16] The Identity Documents Act 2010 (formerly the Identity Cards Act 2006), section 25(5) & (7).
[17] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275784/13-521-identity-related-crime-uk.pdf

The ITADA Achieves Four Things:

- It has made identity theft a separate crime against the individual whose identity was stolen.
- It established the Federal Trade Commission (FTC) as the Federal Government's one point of contact for reporting instances of identity theft by creating the Identity Theft Data Clearinghouse.
- It increased criminal penalties for the offence of identity theft and fraud..
- It recognised "stealing" another personal's personal identifying information as an offence, which till then had made it a crime to only "produce or possess" false identity documents, but not *to* steal another personal's personal identifying information punishable.

Fair Credit Reporting Act, 1970

The Fair Credit Reporting Act,1970 (FCRA) paved the way for the Federal Trade Commission of the USA to create an accurate, fair and private pathway of obtaining and maintaining consumer credit reports. While an individual's credit score in the USA is used to determine a number of things, the Fair Credit Reporting Act focuses on providing rights to an individual associated with that credit score which includes:

- Being informed if the credit report of the individual has been used to deny an application for employment, financial assistance, or insurance;
- Knowing what information is held in the individuals' file;
- Ability to ask what the individuals' credit score is;
- Being able to argue if the information in the individuals' file is inaccurate or incomplete;
- Forcing reporting agencies to remove inaccurate or incomplete information;
- Limiting the access that someone may have to the individuals' file;
- Consenting to provide the individuals' file to other individuals, like an employer;
- Allowing for damages to be received from violators.

Controlling the Assault of Non-Solicited Pornography and Marketing Act, 2003

As the age of the internet advanced, so did spam email messages aimed at tricking individuals into providing their personal information under false pretences. Instead of sharing useful information with individuals who signed up to receive the emails, spam emails including mis-labeled information, viruses, or inappropriate material gained momentum. To help combat the number of spam emails being shared, the Controlling the Assault of Non-Solicited Pornography and Marketing Act, or the CAN-SPAM Act, or was introduced in 2003.

The CAN-SPAM act includes not using subject lines in the emails that are deceptive about the content within the email, the recipient must be able to clearly and easily opt out of receiving such future emails, and if an individual decides to opt out, their name must be removed from the contact list within 10 business days. Punishments for violating the CAN-SPAM Act generally includes fines and considers each separate email that violates the CAN-SPAM act as an independent violation.

Identity Theft Penalty Enhancement Act, 2004

The Identity Theft Penalty Enhancement Act, (ITPEA) was established in 2004, and provides for greater punishment if the individual commits a serious crime using false identification or another individual's identification information. The ITPEA particularly considers "aggravated" identity theft, which includes crimes at the felony level, committing acts of terrorism, or stealing Social Security benefits from another individual. The ITPEA adds punishment time to the sentences of identity theft cases e.g. for felony violations, two additional years in prison can be added on to the sentence, and if a stolen or otherwise false identity was used to carry out a terrorist attack, an additional five years can be added to the overall punishment sentence.

Identity Theft Enforcement and Restitution Act, 2008

As the advent of the internet continued to grow, so did the number of cyber attacks on users' personal identities. But even though identity theft from online sources was becoming a major problem, it was difficult to prosecute someone over an online crime. With the Identity Theft Enforcement and Restitution Act of 2008, (ITERA) certain previous requirements and restrictions that made it difficult to punish cyber crimes were eliminated.

The ITERA allows for various cyber crimes to be considered more seriously and punished more harshly. First, the ITERA makes damaging 10 or more computers a year that are used by the federal government a felony offence. Further the Act also brings other serious crimes into light, including illegal wiretapping, computer fraud, or hacking computer systems. Importantly the ITERA helps victims receive compensation for their time spent dealing with their identity theft case.

Identity Theft Red Flags Rule, 2007

The Identity Theft Red Flags Rule, 2007 (ITRFR) was intended by the US Federal Trade Commission to help individuals, businesses, and organizations keep their eyes open to identity theft "red flags." Under the ITRFR, businesses need to implement a strategy comprised of four basic elements, including how to identify relevant red flags, detect red flags, prevent and mitigate identity theft, and how to update the programme. The ITRFR were updated in 2010 with the Red Flag Clarification Act. Under this Red Flag Clarification Act, professionals like doctors and lawyers who may not receive their full payment amount upfront are excluded from the Red Flags Rule.[18]

PRESENT LAWS IN INDIA RELATING TO IDENTITY CRIME

India presently does not have any specific standalone legislation for offences of identity crime but the Information Technology Act, 2000 along with several provisions in the Indian Penal Code,1860 are primarily used to deal with identity crime offences. As the offence of identity theft has features of both theft and fraud in it, the provisions of fraud, forgery and cheating by impersonation, etc as provided in the Indian Penal Code, 1860 are often invoked along with those of the Information Technology Act, 2000.

Provisions of the Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008

The term identity theft itself was used for the first time in the amended version of the IT Act in 2008. The relevant provisions are as follows:

[18] https://www.idtheftauthority.com/identity-theft-laws/

- Section 66 IT Act: When the fraudster commits hacking with computer system dishonestly or fraudulently.
- Section 66B IT Act: When the fraudster receives any stolen computer resource.
- Section 66C IT Act: Defines Identity Theft to mean, fraudulently or dishonestly making use of the electronic signature, password or any other unique identification feature of any other person.
- Section 66D IT Act: When the fraudster cheats by personation by using computer resource.
- Section 66E IT Act: When the fraudster violates an individuals' Privacy without his or her consent".[19]

The Information technology Act, vide the 2008 amendment now provide punishment for violation of privacy (though the extent is limited) and for cyber terrorism. Women and children are also provided protection under Section 67 A and 67 B of this Act.

Further, stronger laws have been framed to provide protection of "sensitive personal data" in the hands of the intermediaries and service providers (body corporate) thereby though to a limited extent, ensuring data protection and privacy. Exceptional cases where such data can be revealed are, to an agency authorized by the State or Central government for surveillance, monitoring or interception, under Section 69 of the IT Act. The scope of sensitive personal data is defined under the IT Rules, 2011 to mean password, financial information, physical physiological and mental health condition, sexual orientation, medical record and history, and biometric information.

However in India presently, the offence of identity theft attracts many penal provisions of the Indian Penal Code, 1860 as well which are as follows.

Provisions of the Indian Penal Code, 1860

Section 419 IPC: Punishment for Cheating by Personation

When the fraudster by stealing identifying information impersonates the victim to commit fraud or cheating.

Section 420 IPC: Cheating and Dishonestly Inducing Delivery of Property-

When the fraudster deceives the victim into disclosing valuable personal data in the nature of identifiable information which is used later to swindle money from the said victims account.

Section 464 IPC: Making a False Document

When the fraudster dishonestly makes a false document, and also includes instances where the fraudster forges signature of another on any document for gain.

Section 468 IPC: Forgery for Purpose of Cheating

When the fraudster commits forgery for the purpose of cheating and may include forgery which is in the nature of electronic record to lure the victims to pass their identifiable information in order to cheat them.

Section 469 IPC: Forgery for Purpose of Harming Reputation -

When the fraudster commits forgery for the purpose of harming the reputation of an individual.

[19] http://www.neerajaarora.com/identity-theft-or-identity-fraud/

Section 471 IPC: Using as Genuine a Forged Document or Electronic Record

When fraudster fraudulently or dishonestly uses as genuine, the fake document for gain and this includes an electronic record.

Section 474 IPC: Having Possession of Document Described in Section 466 or 467, Knowing it to Be Forged and Intending to Use it As Genuine.-

When the fraudster is in possession of a document known to be forged and intending to use it as genuine and this includes any record of Court or of public register, etc or forgery of valuable security will, etc.

Inadequacy in the Present Indian Laws on Identity Crime and Suggestions on the Way Forward

Though the Information Technology Act, 2000 subsequent to its amendment in 2008 has come a long way in according some protection to data and personal information of an individual from being misused. Still, there are certain facets of the said legislation and laws on identity theft that require further clarity or changes.

To suggest firstly, Section 66 C of the amended The Information Technology Act,2008 protects "unique identification feature", however the meaning of which has not been specified anywhere in the Act. The Information Technology Rules, 2011 has defined the term "sensitive personal information" which needs to be protected by the intermediaries. But it may be too farfetched to attribute the unique identification feature to mean sensitive personal information unless so interpreted by the judiciary or expressly provided for by a legislation.

Secondly to suggest, though the IT Act is applicable to any individual who concerns himself in identity theft involving any computer resource based in India, the jurisdictional issues still remain and cannot be reconciled. Moreso when the accused perpetrator happens to be a non-Indian citizen, and the country of his citizenship has dissimilar laws pertaining to identity theft and has not signed an extradition treaty with India, bringing such a perpetrator to justice in India becomes very difficult.

Thirdly, considering the aspect of compensation to be awarded to the victim, the IT Act proves significantly inadequate. Under the IT Act, the compensation provided under the various provisions are capped and does not consider the situation where a victim might suffer larger loss than this amount specified. Further, as per Section 47 of the IT Act, the Adjudicating Officer is required to consider only into tangible/quantifiable loss caused to the victim while awarding compensation, i.e. whether the amount of gain of unfair advantage, wherever quantifiable, is made as a result of the default, whether the amount of loss caused to any person is as a result of the default and/or the repetitive nature of the default. This results in huge amount of mental trauma and hardship to the victim which he faces as an aftermath of the crime depending upon the subsequent crime to which the unique identification information is put to use. In reality as we all know, it takes much time and resources to regain the lost reputation or to get the credit report corrected, which should have also been considered while awarding compensation.

Fourthly, the quantum of fine provided for identity theft under Section 66 C of the IT Act is up to One lakh only. It needs to be understood that Identity theft is a broader umbrella under which crimes of different intensity can be committed. An identity thief can cause loss of reputation or property to an individual worth some thousand rupees or to a larger population where the loss may amount to millions. Both the cases cannot be considered to be at parity and a minimal token fine not exceeding one lakh is not justified. Further, the other Sections of the Indian Penal Code along with which Section 66 C of the IT Act may normally be clubbed with and applied, do not mention the limit (upper or lower) of fine or the manner in which it should be computed, thus leaving it to the exclusive discretion of the judge.

It is lastly suggested that laws are meant to serve a dual purpose of prevention of a crime and be deterrence. Pre-emption and thereby prevention of identity theft may not be possible.

The deterrence effect could be created in case where generally a certain amount of premeditation or pre thought is invested before its commission in crimes of identity Theft. This could be achieved by imposing stricter punishment and/or fines. Presently, the IT Act makes identity theft a cognizable, bailable and compoundable offence. Infact Section 77 A provides for offences committed under Section 66 C to be compoundable. Further, a three year imprisonment term is too little and will not serve the purpose of deterrence. The provisions being bailable, it might provide an opportunity to the accused to interfere with the investigation of the crime by the cyber cell by tampering with his digital footprints and evidence of his crime.

CONCLUSIONS

It although remains a harsh reality that the present laws in India on identity crime and its implementation are inadequate, the draft Data Protection Report and Bill framed by the Committee of Experts on the Data Protection Framework for India (Chair : Retired Justice B.N. Srikrishna) submitted to the Ministry of Information and Technology, Government of India on November 27, 2017 is a welcome positive first step towards a more robust legal framework in this sphere.

The said Data Protection Bill seeks to administer the "processing" – which includes collecting, recording, adapting, indexing, or even disclosing – of personal data. Personal data in this case is said to refer to any information that is specific to the person, and makes them "identifiable".

The Bill also provides for a category called "sensitive personal data", which includes: passwords, financial data, health data, official identifiers, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex statues, caste or tribe and religious or political beliefs and affiliations.

Essentially, the Bill provides that those intending using personal data in any manner, have to do so in a way that protects the individual's privacy. The Draft Bill then also explains exactly how this is to be done, and who is permitted to do it.

An important facet of this Bill is that **Individuals can give consent** to a person or entity to process their personal data, and such consent should be free, informed, specific, clear and capable of being withdrawn.

The Bill also provides for the **right to be forgotten**, which permits an individual to withdraw consent and request that any data provided to an entity not be disclosed any further. For this to apply, though, an individual will have to make the claim to an Adjudicating Officer, who will then decide whether the demand is fair. This is also unlike the European Union's version of this right, in which the individual can simply demand that their data is erased.

Until we have a robust Data Protection Act, which will contain strong provisions against identity crimes, the following safeguards at an individual level may prove useful in preventing Indentity Crime :

- Protect PIN numbers, never write them on credit/debit cards, or on a slip of paper in a wallet;
- Shield keypads when using ATMs or checkout systems;
- Collect the mail immediately;
- Pay attention to whether bills arrive as scheduled;

- Keep all receipts and account statements;
- Shred unwanted statements or receipts;
- Keep all personal information in a safe place at home;
- Ignore unsolicited requests for personal information;
- Use strong firewalls on home computers;
- Always use secure passwords;
- Check credit reports annually, or any time theft is suspected.[20]

Being cautions in our online activity and adopting safeguards can avoid individuals and organisations from falling prey to the fraudsters of Identity Theft.

REFERENCES

Books

1. *The Information Technology Act 2000.*
2. *Information Technology Amendment Act, 2008.*
3. *Computer, Internet and New Technology Laws – Kanika Seth (2nd Edition published 2016).*
4. *Commentary on Information Technology Act – Apar Gupta (3rd Edition published 2016).*
5. *Data Protection Law in India – Pawan Duggal.*
6. *Larry J. Siegel, E-Study Guide For: Criminology: Theories, Patterns, and Typologies (11 Ed. 2014).*
7. *Fraud Act 2006.*
8. *The Identity Documents Act 2010 (formerly the Identity Cards Act 2006)*
9. *http://www.mazars.co.in/Home/News/Our-Publications/Digitalisation*
10. *http://www.identitytheft.org.uk/*
11. *https://www.actionfraud.police.uk/*
12. *Vivek Tripathi, Cyber Laws India Cyberlawsindia.net,*
13. *http://www.cyberlawsindia.net/index1.html*
14. *https://www.merriam-webster.com/dictionary/identity%20theft*

[20] https://legaldictionary.net/identity-theft/